UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/768,931	01/29/2004	Robert James Demopoulos	14584.1US01	7179

23552 7590 06/24/2008

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
FEARER, MARK D	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/768,931	DEMOPOULOS ET AL.	
	Examiner	Art Unit	
	MARK D. FEARER	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20 March 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's Amendment filed 20 March 2008 is acknowledged.
- Claim 9 has been amended.
- Claims 1-29 are pending in the present application.
- This action is made FINAL.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 20 March 2008 has been considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 24 is rejected under 35 U.S.C. 102(e) as being anticipated by Chesla et al. (US 20040250124 A1).

Consider claim 24. Chesla et al. clearly shows and discloses an intrusion detection system and method comprising a database of event records for each message received within a period of time by a computing system ((“Designating the one of the plurality of parameters as the at least one parameter may include determining the number of occurrences occurred within a certain period of time.”) paragraph 0033 (“FIG. 16 is a block diagram that schematically illustrates components of learning module 66, in accordance with an embodiment of the present invention. Learning module 66 typically comprises a short-term learning module 350 and a long-term learning module 352. In embodiments in which security system 20 is implemented as a network appliance, short-term learning module 350 is typically implemented in the appliance itself. Long-term learning module 352 may be implemented either in the appliance or external to the appliance, for example in a management server using a database.”) paragraph 0245) and event record is identified as a threat by one or more monitor modules on the computing system, each event record including event data provided by the one or more monitor modules that identified the message as a threat ((“A monitoring device monitors network traffic for data addressed to the network objects. Upon detecting a data packet addressed to one of the network objects, packet information is extracted from the data packet. The extracted information is utilized to obtain a set of attack signature profiles corresponding to the network object based on the association data. A virtual processor executes instructions associated with attack signature profiles to determine if the packet is associated with a known network security violation. An attack signature profile generator is utilized to generate additional attack signature

profiles configured for processing by the virtual processor in the absence of any corresponding modification of the virtual processor.") paragraph 0010), the event data including a priority level of the message assigned by one or more monitor modules (("At consistency counter check step 634, controller 500 determines whether the consistency counter is at least T. A positive indication occurs automatically upon entering blocking state 610, since the consistency counter is set to T at step 632. Subsequently, a positive determination indicates that system 20 has experienced stable negative feedback, i.e., an attack has continued, despite filtering, for at least T seconds. In either case, when the consistency counter is greater than or equal to T, the controller checks whether the intensity counter of the highest-ranked source address in the sort buffer exceeds threshold M, at an intensity check step 635. If the controller finds that the intensity counter is less than M, the controller typically returns to misuse state 604, at a transition step 660. (The reason for this transition may be that continued ineffective blocking is pointless, and the sort buffer does not contain additional source addresses that are likely to increase the effectiveness of blocking.) If, however, the controller finds that the intensity counter exceeds M, the controller adds one or more source addresses from the sort buffer to the blocking list, at a blocking list addition step 636. When adding these addresses to the blocking list, the controller generally gives priority to addresses in the sort buffer that have the highest intensity counters, determined as described below with reference to FIG. 22. Source addresses on the blocking list are filtered by filtering module 508, as described hereinbelow. For any given attack, the first time the controller adds source addresses to the blocking list (i.e., immediately upon entering

blocking state 610), the controller typically adds only a single address. When adding additional addresses during the same attack, the controller typically adds two more addresses each time the consistency counter condition is satisfied at step 634.") paragraph 0346), an event type, and data identifying the message's destination (("Common systems used to protect networks at their peripheries include firewalls and intrusion detection systems (IDSs). Firewalls examine packets arriving at an entry to the network in order to determine whether or not to forward the packets to their destinations. Firewalls employ a number of screening methods to determine which packets are legitimate. IDSs typically provide a static signature database engine that includes a set of attack signature processing functions, each of which is configured to detect a specific intrusion type. Each attack signature is descriptive of a pattern which constitutes a known security violation. The IDS monitors network traffic by sequentially executing every processing function of a database engine for each data packet received over a network.") paragraph 0008), data identifying the message's source (("US Patent Application Publications 2002/0107953 to Ontiveros et al. and 2002/0133586 to Shanklin et al., which are incorporated herein by reference, describe a method for protecting a network by monitoring both incoming and outgoing data traffic on multiple ports of the network, and preventing transmission of unauthorized data across the ports. The monitoring system is provided in a non-promiscuous mode and automatically denies access to data packets from a specific source based upon an associated rules table. All other packets from sources not violating the rules are allowed to use the same port. The system provides for dynamic writing and issuing of firewall

rules by updating the rules table. Information regarding the data packets is captured, sorted and cataloged to determine attack profiles and unauthorized data packets.") paragraph 0014), an event identifier (("In an embodiment of the present invention, measuring the time-related property includes observing packets arriving on connections of a stateful protocol. For some applications, analyzing the property includes constructing and analyzing a matrix of packet arrival intensity in the frequency domain, the packet arrival intensity is expressed in terms of a number of the connections. Analyzing the matrix may include identifying as suspect the connections contributing to a high value of the arrival intensity in a region of the matrix. For some applications, determining one or more source addresses of the connections identified as suspect, and blocking the traffic entering the network from the one or more source addresses. The stateful protocol may include a Transmission Control Protocol (TCP).") paragraph 0071), an event description (("Network flood protection module 50 typically sets the baseline portion of each type of packet (UDP, TCP, and ICMP) to the appropriate quota value shown in table 900. Module 50 uses the baseline parameters determined in accordance with table 900 in order to adapt the fuzzy input membership functions, for example as described hereinabove with reference to FIG. 11 in the description of FIS module 62 in network flood module 50.") paragraphs 0440-0441), an event priority (("When adding these addresses to the blocking list, the controller generally gives priority to addresses in the sort buffer that have the highest intensity counters, determined as described below with reference to FIG. 22. Source addresses on the blocking list are filtered by filtering module 508, as described hereinbelow. For any

given attack, the first time the controller adds source addresses to the blocking list (i.e., immediately upon entering blocking state 610), the controller typically adds only a single address. When adding additional addresses during the same attack, the controller typically adds two more addresses each time the consistency counter condition is satisfied at step 634.") paragraph 0346), and a date and time associated with the message (("For some applications, analyzing the property includes detecting a first type of attack, filtering the traffic includes blocking the traffic participating in the attack of the first type, and analyzing the property further includes analyzing the filtered traffic to detect a second type of attack. The method may include filtering the filtered traffic in order to block the traffic participating in the attack of the second type. Alternatively or additionally, analyzing the filtered traffic includes: measuring a time-related property of the filtered traffic; transforming the time-related property of the filtered traffic into a frequency domain; and analyzing the property in the frequency domain in order to detect the attack of the second type. The first type of attack may include a network flood attack, and the second type of attack includes a stateful protocol attack.) paragraph 0046).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-4, 8-9 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Bhattacharya et al. (US 20040133672 A1).

Consider claims 1 and 9. Chesla et al. discloses a method of identifying threats to a computing system received from a network, the computing system having a plurality of monitor modules including a first monitor module, comprising: evaluating a

message received from the network with the plurality of monitor modules and identifying the message as a threat by one or more monitor modules ((“Common systems used to protect networks at their peripheries include firewalls and intrusion detection systems (IDSs). Firewalls examine packets arriving at an entry to the network in order to determine whether or not to forward the packets to their destinations. Firewalls employ a number of screening methods to determine which packets are legitimate. IDSs typically provide a static signature database engine that includes a set of attack signature processing functions, each of which is configured to detect a specific intrusion type. Each attack signature is descriptive of a pattern which constitutes a known security violation. The IDS monitors network traffic by sequentially executing every processing function of a database engine for each data packet received over a network.”) paragraph 0008). However, Chesla et al. fails to disclose receiving event data from said modules, storing event data in a database comprising pre-existing events, comparing current event data with pre-existing event data, or taking action in response to event data. Bhattacharya et al. discloses receiving event data from the one or more monitor modules, the event data related to the message ((“In order to overcome the deficiency discussed above, multiple security devices such as intrusion detection sensors (IDS) are deployed at different sections of a computer network to detect multiple security-related events simultaneously. As shown in FIG. 1, security devices are attached to routers, firewalls, switches and hosts, etc. Each security device is configured such that whenever it detects a suspicious event, e.g., an IP packet, it sends an event message to a network security monitor. The network security monitor is

responsible for correlating diverse events from different parts of the network and providing insights into higher-level attack scenarios.") paragraph 0005); storing the event data in a first event record in a database on the computing system, the database including a plurality of second event records containing event data related to previous messages; (("For various reasons, the data and traffic volume associated with security events have increased dramatically over time. For example, a large number of intrusions can be automated and launched simultaneously from geographically dispersed locations, network link speed is increasing, security devices are becoming faster and generating more data, and single attack can cause multiple events to be generated from various security devices that lie on different network topological paths of that attack. Databases have been used to store this large volume of event messages, and different queries have been designed to correlate multiple event messages in order to detect a high-level attack.") paragraph 0006 ("When receiving a new event message, the message is compared with the constraint of a leaf node. If there is a match, this message is associated with the leaf node; if not, the messages are compared with the constraint of a next leaf node, if any. When a match is found, data representing the event message is stored in a value set associated with the identified leaf node. If a new value set is required for this event message, a new partial solution pointing to the value set is created. When a new event message is associated with a leaf node, the parent node of the leaf node, a non-leaf node, is invoked for further processing.") paragraph 0011); analyzing, after receipt of event data from any one of the plurality of monitor modules, the first event record and second event records in the database (("Therefore,

it would be highly desirable to have a method and apparatus that can correlate event messages in real time as event messages arrive at a network security monitor, and to thereby detect in real time security attacks involving multiple events, even when the attacks include packets sent by multiple distinct sources.") paragraph 0007); and transmitting a command to the first monitor module, in response to results of the analysis, the command including at least some event data from the first event record and a security action to be taken by the first monitor module (("Upon invocation by one of its child nodes, a non-leaf node retrieves event messages from those corresponding leaf nodes through their partial solution links and applies the retrieved event messages to the inter-event constraint associated with the non-leaf node. If the inter-event constraint is satisfied, the method generates a new partial solution and associates it with the non-leaf node. If the non-leaf node is the root node of the decision graph, the partial solution is further converted into a complete solution to the correlation rule and certain appropriate actions will be taken.") paragraph 0013).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate receiving event data from modules, storing event data in a database comprising pre-existing events, comparing current event data with pre-existing event data, and taking action in response to event data as taught by Bhattacharya et al. with a method of identifying threats to a computing system received from a network, the computing system having a plurality of monitor modules including a first monitor module, comprising: evaluating a message received from the network with the plurality of monitor modules and identifying the message as a threat

by one or more monitor modules as taught by Chesla et al. for the purpose of intrusion detection.

Consider claim 2, and as applied to claim 1 above. Chesla et al., as modified by Bhattacharya et al., discloses a method wherein event data includes information identifying a message (("... identifying the one or more source IP addresses participating in the attack by counting the misused connections per each of the plurality of source IP addresses.") Chesla et al., paragraph 0076), a type of threat potentially posed by a message ("IDSs typically provide a static signature database engine that includes a set of attack signature processing functions, each of which is configured to detect a specific intrusion type. Each attack signature is descriptive of a pattern which constitutes a known security violation.") Chesla et al., paragraph 0008), and an indication of a relative priority for a message (("When adding these addresses to the blocking list, the controller generally gives priority to addresses in the sort buffer that have the highest intensity counters, determined as described below with reference to FIG. 22.") Chesla et al., paragraph 0346).

Consider claim 3, and as modified by claim 1 above. Chesla et al., as modified by Bhattacharya et al., discloses a method wherein an action to be taken by a monitor module is to block all future messages identified by event data (("Upon detection of an attack, the network security system determines characteristic parameters of the anomalous traffic, and then filters new traffic entering the network using these parameters. The system uses a feedback control loop in order to determine the effectiveness of such filtering, by comparing the expected and desired results of the

filtering. Based on the feedback, the system adjusts the filtering rules appropriately, so as to generally optimize the blocking of malicious traffic, while minimizing the blocking of legitimate traffic. The security system typically uses these techniques for protecting against stateless DoS or DDoS network flood attacks, such as UDP, ICMP, and stateless SYN flood attacks.") Chesla et al., paragraph 0017).

Consider claim 4, and as applied to claim 1 above. Chesla et al., as modified by Bhattacharya et al., discloses a method wherein analyzing first and second event records in a database comprises identifying the second event records that relate to the first event record; and calculating a relative threat level for the message based on the second event records that relate to the first event record (("In an embodiment of the present invention, analyzing the property includes determining at least one baseline characteristic of the traffic, and adapting the at least one fuzzy logic algorithm responsively to the baseline characteristic. For some applications, determining the at least one baseline characteristic includes applying Infinite Impulse Response (IIR) filtering to at least one parameter of the traffic. Determining the at least one baseline characteristic may include determining separate baseline characteristics for each hour of a week.") Chesla et al., paragraph 0048).

Consider claim 8, and as applied to claim 1 above. Chesla et al., as modified by Bhattacharya et al., discloses a method wherein a security action is a security action that the filter (read as first monitor) module did not perform based on the filter module's internal evaluation of the message (("If the attack level has not changed, however, the controller increments the hierarchy counter, at an increment counter step 116. Because

the attack level has not changed, the controller assumes that the same attack is continuing, but that the intensity of the current filtering is insufficient for effective attack prevention. The method returns to step 106, at which the trapping module again determines signatures, in case they have changed since the last determination. Filtering module 70 applies stricter filtering rules, responsively to the higher counter, at step 110. This feedback loop continues to tighten the filtering, if necessary, until the hierarchy counter reaches its maximum value, which is typically equal to the number of different signature types available, as described hereinbelow with reference to FIGS. 17A and 17B. If the filtering remains ineffective after these iterations, the controller typically directs the filtering module to take more drastic traffic blocking steps, such as blocking all traffic of a certain protocol, to a certain port, or from a certain IP address.") Chesla et al., paragraph 0136).

Consider claim 14, and as applied to claim 9 above. Chesla et al., as modified by Bhattacharya et al., discloses a method of monitoring communication traffic wherein the calculating operation is repeated after each receipt of new event data from one of the plurality of computing systems (("In step 708, node N first traverses down the decision tree to a value set through a chain of partial solutions starting from a partial solution associated with one child node of N and then retrieves a combination of relevant event parameter values associated with that value set. This procedure repeats itself for every child node's partial solution and produces multiple sets of relevant event parameter values in association with node N.") Bhattacharya et al., paragraph 0078).

Consider claim 15, and as applied to claim 14 above. Chesla et al., as modified by Bhattacharya et al., discloses a method of monitoring communication traffic wherein calculating further comprises identifying pre-existing event data that relate to the new event data, and determining if the identified pre-existing event data indicate that the threat posed by the message is greater or lesser than relevant event parameter values (("If the new event message satisfies the intra-event constraint of a leaf node (605-Yes), the process moves to step 613. In step 613, the process checks the event parameters of the incoming message against value sets associated with the leaf node, if any. The checking result has two possibilities, either there is an existing value set that shares the same combination of relevant event parameter values as the incoming event message or there is no such value set.") Bhattacharya et al., paragraph 0069).

Claims 17 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (US 20020087882 A1) in view of Chesla et al. (US 20040250124 A1).

Consider claim 17. Schneier et al. discloses a method for deleting messages received by a computing system from a network comprising: receiving a message in a queue (read as buffer) on the computing system, the message directed to a destination on the computing system (("Message flow through Pipes 3000 can be controlled by means of (i) a client program or process running on the probe/sentry end to service queues of incoming messages from and outgoing messages to the SOC;") paragraph 0040); evaluating the message with a plurality of monitor modules (("The present invention offers methods and systems for dynamic network intrusion monitoring,

detection and response. In an exemplary implementation, these methods and systems may be used to deploy and provide a managed security monitoring service (the "MSM service") that monitors a customer's network activity using a probe or "sentry" system, collects status data from monitored components, filters or otherwise analyzes the collected data for activity possibly implicating security concerns, alerts and transmits information about such activity to trained security analysts working at secure operations centers ("SOCs"), and then guides the security analysts and customer through an appropriate response (with appropriate follow-up, if necessary).") paragraph 0005); storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority; and analyzing event records in the database (("In an exemplary embodiment, security analysts at a SOC work in concert with the "SOCRATES".sup.1 problem and expertise management system to categorize, prioritize, investigate and respond to customer incidents or "problems." The SOCRATES system, among other things, collects and formats gateway messages into "problem tickets" (each of which represents a discrete security-related event or incident of possible intrusive activity happening on a customer's network), associates with each such ticket information useful for problem investigation, resolution and response, presents such tickets to security analysts for handling, and generally serves as a repository of useful information and procedures. Preferably, in the process of orchestrating the management of problem tickets, the SOCRATES system continuously augments problem-solving tools such as tables which

tie symptoms to technology, symptoms to diagnosis, or vulnerability to diagnosis. This continuous improvement allows the invention to take full advantage of specialized nature of the monitoring system. .sup.1 "SOCRATES" is an acronym standing for Secure Operations Center Responsive Analyst Technical Expertise System.") paragraph 0021 ("In an exemplary implementation, the expertise, knowledge and capabilities of MSM service security analysts can be supplemented by a variety of knowledge databases containing detailed information helpful for investigating, evaluating and responding to incidents. Security intelligence databases can contain information about, among other things, the characteristics of various network hardware and software products, known vulnerabilities of such products, the use and characteristics of various hacker tools, and known effective and ineffective responses to various kinds of attacks. Such databases could be continually updated by the MSM service by, for example, monitoring hacker forums, reviewing security analysts' incident reports, and evaluating customer audit data for new attack footprints.") paragraph 0013); and selectively deleting the message from the buffer before delivery to the destination (("... possible functions of such a gateway system are (1) to reformat, add, or delete information to incoming messages from the probe/sentry systems ("sentry messages") to ensure maximum utility of the output "gateway messages"") paragraph 0019). However, Schneier et al. fails to disclose if the message is identified as a potential threat by one or more of the monitor modules. Chesla et al. discloses a method of identifying threats to a computing system received from a network, the computing system having a plurality of monitor modules including a first monitor

module, comprising: evaluating a message received from the network with the plurality of monitor modules and identifying the message as a threat by one or more monitor modules ("Common systems used to protect networks at their peripheries include firewalls and intrusion detection systems (IDSs). Firewalls examine packets arriving at an entry to the network in order to determine whether or not to forward the packets to their destinations. Firewalls employ a number of screening methods to determine which packets are legitimate. IDSs typically provide a static signature database engine that includes a set of attack signature processing functions, each of which is configured to detect a specific intrusion type. Each attack signature is descriptive of a pattern which constitutes a known security violation. The IDS monitors network traffic by sequentially executing every processing function of a database engine for each data packet received over a network.") paragraph 0008).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method of identifying threats to a computing system received from a network, the computing system having a plurality of monitor modules as taught by Chesla et al. with a method for deleting messages received by a computing system from a network comprising: receiving a message in a queue on the computing system, the message directed to a destination on the computing system; evaluating the message with a plurality of monitor modules; storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority; and

analyzing event records in the database; and selectively deleting the message from the buffer before delivery to the destination as taught by for the purpose of dynamic network intrusion monitoring.

Consider claim 21, and as applied to claim 17 above. Schneier et al., as modified by Chesla et al., discloses a method for deleting messages received by a computing system from a network further comprising transmitting a command to a security device to automatically delete future messages in the buffer having specified event data for a specified period of time ((“… delete information to incoming messages from the probe/sentry systems ("sentry messages") to ensure maximum utility of the output "gateway messages" …") Schneier et al., paragraph 0019 (“Escalations may be of various types, including time-based and event-driven. Time-based escalations can be intended to capture problems that have remained in a particular state beyond a specified period of time. Event-based escalations can be designed to trigger immediately when a predefined condition is met. When escalation criteria are met, workflow procedures can be defined to perform one or more actions.”) Schneier et al., paragraph 0099).

Consider claim 22, and as applied to claim 17 above. Schneier et al., as modified by Chesla et al., discloses a method for deleting messages received by a computing system from a network further comprising transmitting a command to a security device to automatically delete future messages in the buffer capable of being sent to a specified port ((“… delete information to incoming messages from the probe/sentry systems ("sentry messages") to ensure maximum utility of the output "gateway

messages" ...") Schneier et al., paragraph 0019 ("An exemplary architecture for Pipes 3000 is as follows. A process on the probe/sentry runs as root. This process can keep its control information in a certain directory. To send a message, another process on the probe/sentry can send this root process a Transmission Control Protocol ("TCP") connection on, for example, 127.0.0.1 port XYZ and emit a message in "Pipes User Message Format." A response may then be sent back to the Pipes client indicating success, failure, or enqueued. The Pipes client can maintain a context for the SOC to which it is currently connected. Possible states include "connected" and "attempting to connect." Preferably, the Pipes client should always be connected to a SOC (or attempting to connect). The Pipes client also preferably runs a loop with selects and sleeps such that it processes input from its SOC and from clients on the local machine. The root process running on the probe/sentry can use, for example, port 443 to behave as a normal TLS (SSL) client and can also listen on port 468 ("photuris"). The root process should be started before everything else, so the probe/sentry filtering subsystem can talk to it. A process running on the gateway should listen to port 443. When it gets a call, it should fork a child process that handles the probe/sentry. There should therefore be one process per probe/sentry, although each gateway might be associated with a few hundred or more probe/sentries. There should also be a port 468 connection to the probe/sentry system communications and resource coordinator.") Schneier et al., paragraph 0041).

Consider claim 23, and as applied to claim 17 above. Schneier et al. discloses a method for deleting messages received by a computing system from a network further

comprising event data including an event type, an event description, and an event timestamp (("SOCRATES 6000 can generate a variety of reports for customers or internal use through report generation module 6040. For example, a current report may be sent to and accessed directly from probe/sentry system 2000. This report can be web-based and can include the status of the probe/sentry system, the status of open tickets and detailed log information. A weekly report could include incident summaries, open ticket summaries, details on critical and suspicious events, and sensor reports, and could be emailed to the primary customer contact. The weekly report could also include trend analysis of data covering monthly, quarterly and "to-date" data collections and could contain a variety of report sections, including ticket summary (including accumulation of events by type for the week, month, quarter, year), critical tickets summary, top ten events (including weekly, monthly, broken down by event type), known attackers list, top ten targets list, IP watch list (including attack occurrences broken down by day and time), probe/sentry statistics, and known device list.") paragraph 0061). However, Schneier et al. fails to disclose an indication of the source of the message, and an indication of the destination of the message. Chesla et al. discloses a network protection apparatus comprising monitoring data packet fields ("For some applications, the traffic includes packets having packet header fields, and the at least one parameter includes a value of one of the packet header fields. The one of the packet header fields may be selected from a list consisting of: Transmission Control Protocol (TCP) sequence number, Internet Protocol (IP) identification number, source port, source IP address, type of service (ToS), packet size, Internet Control Message

Protocol (ICMP) message type, destination undefined port, destination undefined IP address, destination defined port, destination defined IP address, time-to-live (TTL), and transport layer checksum. Alternatively or additionally, the traffic includes packets having payloads, and the at least one parameter includes a value of one of the packet payloads.") paragraph 0045).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a network protection apparatus comprising monitoring data packet fields as taught by Chesla et al. with a method for deleting messages received by a computing system from a network further comprising event data including an event type, an event description, and an event timestamp as taught by Schneier et al. for the purpose of traffic matching network monitoring.

Claims 5, 7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Bhattacharya et al. (US 20040133672 A1) and in further view of Lin et al. (US 6405250 B1).

Consider claims 5 and 16, and as applied to claims 4 and 15, respectively. Chesla et al., as modified by Bhattacharya et al., discloses a method of intrusion detection comprising analyzing a plurality of event records in a database. However, Chesla et al., as modified by Bhattacharya et al., fails to disclose a method comprising a Bayesian analysis. Lin et al. discloses trend analyzing passive network monitoring comprising Bayesian probability ((“Trend analyzer 402 determines likely causes based on a Bayesian belief network that accounts for the operating status of other network elements; this is done at step 731. Trend analyzer 402 then forwards the reasoning

outcome, also in the form of a set of potential transitions, at step 702 to action chooser 403.") column 9 lines 29-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate trend analyzing passive network monitoring comprising Bayesian probability as taught by Lin et al. with a method of intrusion detection comprising analyzing a plurality of event records in a database as taught by Chesla et al., as modified by Bhattacharya et al., for the purpose of formulating state transition models.

Consider claim 7, and as applied to claim 4 above. Chesla et al., as modified by Bhattacharya et al., discloses a method of intrusion detection comprising transmitting a command in response to a security threat. However, Chesla et al., as modified by Bhattacharya et al., fails to disclose a method wherein an interface is used to help determine a necessary security action. Lin et al. discloses a blocking rate comprising distribution traffic of an interface that is used to determine requirements (("Consider again the simple behavior transition model depicted in FIG. 3 as an example. We can associate with State 301 an option of reporting throughput and blocking rate every 15 minutes. On the other hand, in a slightly overload situation in State 302, we may be interested in the percentage distribution of traffic entering an NE through different interfaces. We may also like to know the blocking rate of at each individual interface to determine if a particular admission policy is working properly. Therefore, we can associate with State 302 an option of reporting throughput and blocking rate respectively on a per interface basis, properly still every 15 minutes. State 303

represents either internal or external network problems. If the problem is within an NE, the NE may want to report its recovery progress. However, if the problem is likely to be outside of the NE, NMS 120 may only need to know from the NE how much traffic it is sending to its neighboring. NE's. Therefore, there could be multiple options associated with State 303. This is where a collaborative decision between NMS and each NE is preferred.") column 7 lines 7-26)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a blocking rate comprising distribution traffic of an interface that is used to determine requirements as taught by Lin et al. with a method of intrusion detection comprising transmitting a command in response to a security threat as taught by Chesla et al., as modified by Bhattacharya et al., for the purpose of ranking threat activity on a network.

Claims 6 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Bhattacharya et al. (US 20040133672 A1) and in further view of Snapp (US 20030172064 A1).

Consider claims 6 and 13, and as applied to claims 1 and 9, respectively. Chesla et al., as modified by Bhattacharya et al., discloses an intrusion detection system comprising first and second event records in a database. However, Chesla et al., as modified by Bhattacharya et al., fails to disclose a method of deleting an event from a database dependent upon the age of the event. Snapp discloses a method of updating a database comprising a step of removing from an update file information that has an age in excess of a specified period of time ((“In accordance with another embodiment

of the present invention, a method for updating information contained in a database comprising … the step of removing from the update file information that has an age in excess of a specified period of time.") paragraph 0012).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method of updating a database comprising a step of removing from an update file information that has an age in excess of a specified period of time as taught by Snapp with an intrusion detection system comprising first and second event records in a database as taught by Chesla et al., as modified by Bhattacharya et al., for the purpose of database updating.

Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Bhattacharya et al. (US 20040133672 A1) and in further view of James et al. (US 6993022 B1).

Consider claims 10 and 11, and as applied to claims 9 and 10, respectively. Chesla et al., as modified by Bhattacharya et al., discloses an intrusion detection system comprising multiple leaf nodes of a decision tree. However, Chesla et al., as modified by Bhattacharya et al., fails to disclose a first and a second computing system wherein each system comprises a plurality of nodes. James et al. discloses an apparatus for mapping communications through a router between nodes on different buses within a network of buses comprising a first plurality of nodes and a second plurality of nodes (("In yet another aspect of the present invention, a network of devices includes a first bus including a first plurality of nodes, a second bus including a second plurality of nodes and a routing device coupled to the first bus and the second bus. The

routing device includes a receiving circuit configured to receive a communication from one of the first plurality of nodes, the communication including an address value having a bus number and a node number, together forming an address of the routing device, and a routing value used to determine an address of a targeted one of the second plurality of nodes, a parsing circuit coupled to the receiving circuit to extract the routing value from the address value within the communication, a remapping circuit coupled to the parsing circuit to obtain the routing value from the parsing circuit and remap the address value of the communication thereby forming a remapped communication with a remapped address value corresponding to the address of the targeted one of the second plurality of nodes and a transmitting circuit coupled to the remapping circuit and configured to transmit the remapped communication with the remapped address on the second bus to the targeted one of the second plurality of nodes. The communication and the remapped communication are bus packets. Preferably, the routing value includes the address of the targeted one of the second plurality of nodes and an offset value within memory space of the targeted one of the second plurality of nodes. The remapping circuit includes a routing table. Alternatively, the routing device as claimed in claim 27 wherein the remapping circuit utilizes a table index value within the routing value to obtain the address of the targeted one of the second plurality of nodes from a location within the routing table corresponding to the table index value. Preferably, the first and second buses both substantially comply with a version of an IEEE Std 1394 standard.") column 4 lines 41-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate an apparatus for mapping communications through a router between nodes on different buses within a network of buses comprising a first plurality of nodes and a second plurality of nodes as taught by James et al. with an intrusion detection system comprising multiple leaf nodes of a decision tree as taught by Chesla et al., as modified by Bhattacharya et al., for the purpose of parallel resources.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Bhattacharya et al. (US 20040133672 A1) and in further view of Eshghi et al. (US 20020165954 A1).

Consider claim 12, and as applied to claim 9 above. Chesla et al., as modified by Bhattacharya et al., discloses an intrusion detection system comprising multiple leaf nodes of a decision tree. However, Chesla et al., as modified by Bhattacharya et al., fails to disclose an intrusion detection system wherein event messages contain data identifying action from a second computing device. Eshghi et al. discloses a system for monitoring browser event activities wherein events comprise identification for sending monitored data to a measurement computer (("An alternative embodiment of the present invention is directed to a system and method for monitoring events on a network computer, including downloading a web page from a web server to a client browser within a network, wherein the web page includes a script tag identifying a location of a monitoring function; retrieving the monitoring function based on information in the script tag; invoking the monitoring function to monitor an event on the client

browser; and sending monitored data to a measurement computer, wherein the measurement computer is a computer other than the web server.") paragraph 0011).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a system for monitoring browser event activities wherein events comprise identification for sending monitored data to a measurement computer as taught by Eshghi et al. with an intrusion detection system comprising multiple leaf nodes of a decision tree as taught by Chesla et al., as modified by Bhattacharya et al., for the purpose of collaborative network event monitoring.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (US 20020087882 A1) in view of Chesla et al. (US 20040250124 A1) and in further view of Snapp (US 20030172064 A1).

Consider claim 18, and as applied to claim 17 above. Schneier et al., as modified by Chesla et al., discloses a method for deleting messages from an event record database. However, Schneier et al., as modified by Chesla et al., fails to disclose a method comprising deleting from a database previous event records that are older than a specified age. Snapp discloses a method of updating a database comprising a step of removing from an update file information that has an age in excess of a specified period of time (("In accordance with another embodiment of the present invention, a method for updating information contained in a database comprising ... the step of removing from the update file information that has an age in excess of a specified period of time.") paragraph 0012).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method of updating a database comprising a step of removing from an update file information that has an age in excess of a specified period of time as taught by Snapp with a method for deleting messages from an event record database as taught by Schneier et al., as modified by Chesla et al., for the purpose of database updating.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (US 20020087882 A1) in view of Chesla et al. (US 20040250124 A1) and in further view of Bhattacharya et al. (US 20040133672 A1).

Consider claim 19, and as applied to claim 17 above. Schneier et al., as modified by Chesla et al., discloses a method for deleting messages from an event record database. However, Schneier et al., as modified by Chesla et al., fails to disclose a method for deleting messages from an event record database wherein a determining operation is repeated each time a new event record is received. Bhattacharya et al. discloses a method of monitoring communication traffic wherein the calculating operation is repeated after each receipt of new event data from one of the plurality of computing systems ((“In step 708, node N first traverses down the decision tree to a value set through a chain of partial solutions starting from a partial solution associated with one child node of N and then retrieves a combination of relevant event parameter values associated with that value set. This procedure repeats itself for every child node's partial solution and produces multiple sets of relevant event parameter values in association with node N.”) paragraph 0078) and calculating further comprises

identifying pre-existing event data that relate to the new event data, and determining if the identified pre-existing event data indicate that the threat posed by the message is greater or lesser than relevant event parameter values ("If the new event message satisfies the intra-event constraint of a leaf node (605-Yes), the process moves to step 613. In step 613, the process checks the event parameters of the incoming message against value sets associated with the leaf node, if any. The checking result has two possibilities, either there is an existing value set that shares the same combination of relevant event parameter values as the incoming event message or there is no such value set.") paragraph 0069).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method of monitoring communication traffic wherein the calculating operation is repeated after each receipt of new event data from one of the plurality of computing systems as taught by Bhattacharya et al. with a method for deleting messages from an event record database as taught by Schneier et al., as modified by Chesla et al., for the purpose of integrated data traffic monitoring.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (US 20020087882 A1) in view of Chesla et al. (US 20040250124 A1) in further view of Bhattacharya et al. (US 20040133672 A1) and in further view of Lin et al. (US 6405250 B1).

Consider claim 20, and as applied to claim 19 above. Schneier et al., as modified by Chesla et al. and Bhattacharya et al., discloses a communications monitoring method wherein an existing value set has relevant event parameter values matching

relevant parameter values of a current event message. However, Schneier et al., as modified by Chesla et al. and Bhattacharya et al., fails to disclose a method of identifying event records in a database that relate to the new event record comprising a Bayesian analysis. Lin et al. discloses trend analyzing passive network monitoring comprising Bayesian probability (("Trend analyzer 402 determines likely causes based on a Bayesian belief network that accounts for the operating status of other network elements; this is done at step 731. Trend analyzer 402 then forwards the reasoning outcome, also in the form of a set of potential transitions, at step 702 to action chooser 403.") column 9 lines 29-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate trend analyzing passive network monitoring comprising Bayesian probability as taught by Lin et al. with a communications monitoring method wherein an existing value set has relevant event parameter values matching relevant parameter values of a current event message as taught by Schneier et al., as modified by Chesla et al. and Bhattacharya et al., for the purpose of formulating state transition models.

Claims 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Noda et al. (US 6816890 B2).

Consider claims 25 and 26, and as applied to claim 24 above. Chesla et al. discloses a database of event records comprising threat level, identifier, type, description, priority, timestamp, source, and destination information. However, Chesla et al. fails to disclose a database of event records comprising a message source and

destination IP address, port, or URL, or whether message source was internal to computing system. Noda et al. discloses an L2TP access concentrator comprising message source and destination IP addresses, ports, and URLs, and whether a message source was internal to computing system ((“FIG. 22A shows a packet transfer sequence used in the case where contents data designated by an URL exists in the Web cache server 113 in the second embodiment, and FIG. 22B shows the relation between the destination address DA and the source address SA of an IP header attached to each of transfer packets illustrated in FIG. 22A.”) column 17 lines 48-53 (“The protocol processor 81 adds an internal header 1010 including internal routing information to the packet (a PPP frame 1103 to which the PPP connection ID 1001 is added) received from the interface 80 (80A to 80C) and outputs the resultant to the internal switch unit 87. The PPP connection ID 1001 added to the received packet is rewritten by the protocol processor 81 as necessary. The internal switch unit 87 switches the received packet from a protocol processor 81 to another protocol processor 81 designated by the internal routing information (internal header) 1010.”) column 12 lines 61-67 and column 13 lines 1-3 (“When the upper layer protocol is the IP, the destination port number of the TCP/UDP header is checked. If the destination port number is, for example, "80" as a well-known port number of the HTTP, in order to transfer the received packet (HTTP request message) to the cache server 113, a destination IP address converting process 1509 is executed to rewrite the destination address of the IP header to an IP address value of the Web cache server. The received packet subjected to the address conversion is transmitted to the internal switch unit 87

in a form that the internal routing information 1010 designating the cache server protocol processor 81B is added in front of the PPP connection ID 1001. In a manner similar to the first embodiment shown in FIG. 15, the packet is transferred as the IP packet 702 to the cache server 113 via the cache server protocol processor 81B.") column 19 lines 14-29).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate an L2TP access concentrator comprising message source and destination IP addresses, ports, and URLs, and whether a message source was internal to computing system as taught by Noda et al. with a database of event records comprising threat level, identifier, type, description, priority, timestamp, source, and destination information as taught by Chesla et al. for the purpose of event routing.

Claims 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 20040250124 A1) in view of Mathews et al. (US 20030061256 A1).

Consider claims 27 and 28, and as applied to claims 24 and 27, respectively. Chesla et al. discloses a database of event records comprising threat level, identifier, type, description, priority, timestamp, source, and destination information. However, Chesla et al. fails to disclose a database wherein event data includes data identifying the computing system that received the message, or the event data includes data identifying any actions taken by monitor modules on the computing system upon receipt of the message. Mathews et al. discloses an apparatus for adaptive transaction processing between uniform information services and applications wherein resource

service providers (read as modules) are identified for target transactions and the results of an operation and content description are returned upon execution (("In the present invention, networked services providing or consuming information are classified according to a uniform service model (USM), where the service and information they provide can be quantitatively described as to function, type of information, access model using a standardized taxonomic structure. With this classification, the present invention provides a method and system for allowing such classified services to conduct transactions with other services without explicitly identifying the source or targets of the transaction. Services qualified as Resource Service Consumer (RSC) submit transaction definitions (TDs) to a TPF (or system of TPFs as provided by a particular configuration) in the context of a session, where upon the TPF analyzes the TD in order to determine the set of services to use and additional information that is required prior to execution. Once the TD services are selected and associated transaction situation context (TSC) defined, the TPF executes the transaction either synchronously or asynchronously as defined by the TD. During transaction processing, the TPF may execute multiple operations with resource service providers (RSP) combining the results of the operations as needed. The results of these operations are resources, which may be information content or descriptions of information or services thereof.") paragraph 0060).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate an apparatus for adaptive transaction processing between inform information services and applications wherein resource

service providers are identified for target transactions and the results of an operation and content description are returned upon execution as taught by Mathews et al. with a database of event records comprising threat level, identifier, type, description, priority, timestamp, source, and destination information as taught by Chesla et al. for the purpose of adaptive transaction processing.

Consider claim 29, and as applied to claim 24 above. Chesla et al. discloses a database of event records comprising threat level, identifier, type, description, priority, timestamp, source, and destination information. However, Chesla et al. fails to disclose a database wherein event data is provided in disparate forms by monitor modules and stored in a standardized form in an event record. Mathews et al. discloses an apparatus for adaptive transaction processing between uniform information services and applications wherein the benefits of transformation between raw form data and disparate information is taught ("At an increasing rate, more and more information is being made available `on-line`, whether publicly through portals and other web sites or via secured access to corporate intranets. On-line access means users can quickly get at information from any networked device as long as it supports the appropriate application protocols. Most of this information is accessible through some pre-defined interface, which allows users to interact with the information in a controlled fashion: including functions for security, utilization, billing, etc. To date, most of these information services provide their information in a customized and non-standard form, requiring specialized applications (including web pages) software to work with it. Though the

information may have value in its `raw` form, the potential value for integrating disparate information services has many more benefits.") paragraph 0004).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate an apparatus for adaptive transaction processing between uniform information services and applications wherein the benefits of transformation between raw form data and disparate information is taught as taught by Mathews et al. with as taught by for the purpose of on-line user access.

Response to Arguments

Applicant's arguments filed May 7, 2007 with respect to claims 1, 9, 17, and 24-29 have been considered.

Claim 24

Applicant argues that Chesla et al. does not disclose a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising an intrusion detection database of threat types (paragraphs 0008 and 0245); a real-time statistics module that receives raw, unfiltered traffic arriving from a WAN (paragraphs 0084, 0087 and 0242); a method of determining the number of

occurrences occurring within a certain period of time (paragraph 0033); and a profiler defining old and new threats (paragraphs 0010-0011, 0014 and 0016).

Applicant argues that Chesla et al. does not disclose event records having event data provided by the one or more monitor modules that identified the message as a threat and including the various claimed data elements (event identifier, event type, event description, etc.). The Examiner respectfully disagrees. Chesla et al. discloses a method of analyzing an attack to the packet level, comprising Transmission Control Protocol (TCP) sequence number, Internet Protocol (IP) identification number, source port, source IP address, type of service (ToS), packet size, Internet Control Message Protocol (ICMP) message type, destination undefined port, destination undefined IP address, destination defined port, destination defined IP address, time-to-live (TTL), and transport layer checksum. Alternatively or additionally, the traffic includes packets having payloads, and the at least one parameter includes a value of one of the packet payloads (paragraphs 0045-0046), and a controller comprising a blocking list that gives priority to addresses in the sort buffer that have the highest intensity counters (paragraph 0346).

Applicant argues that none of the cited portions of Chesla et al. collect information into a common event record for storage in a database, or receipt of such data from a monitor module. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack a statistics module 64 to collect baseline statistics regarding traffic parameters (paragraph 0131); and a method for protecting a network from an attack comprising a plurality of monitoring modules

(paragraphs 0140, 0170 and 0207).

Claim 1

Applicant argues that combination of Chesla et al. and Bhattacharya et al. at least fails to disclose storing event data related to the message as an event record in a database containing second event records containing event data related to previous messages and analyzing the event record and the second event records in the database. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising comparing attack types of a first and a second type (paragraphs 0046 and 0053-0055).

Claim 9

Applicant argues that combination of Chesla et al. and Bhattacharya et al. at least fails to disclose storing the new event data at the security facility in an event database that includes pre-existing event data, and calculating, at the security facility and based on the new and pre-existing event data in the event database, a network threat level for the message. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising an existing baseline of threats and new, detected incoming threats at a learning module that analyzes the threat (paragraph 0131).

Claim 17

Applicant argues that The combination of Schneier et al. and Chesla et al. fails to teach or suggest "if the message is identified as a potential threat by one or more of the monitor modules, storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority; and analyzing event records in the database." The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a plurality of monitoring modules (paragraphs 0140, 0170 and 0207); an attributed type pf threat (paragraph 0008); a controller comprising a blocking list that gives priority to addresses in the sort buffer that have the highest intensity counters (paragraph 0346); and a database comprising new and old threats (paragraphs 0131 and 0245).

Applicant argues that Schneier fails to disclose or suggest storing event records in a database which include a threat type. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a database of threats (paragraph 0245); an existing baseline of threats and new, detected incoming threats at a learning module that analyzes the threat (paragraph 0131).

Applicant argues that Schneier et al. fails to disclose storing the output of the monitor modules related to a potential threat message in a new event record in a

database containing a plurality of previous event records. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a database of threats (paragraph 0245); an existing baseline of threats and new, detected incoming threats at a learning module that analyzes the threat (paragraph 0131).

Claims 25-26 and 27-29

Applicant argues that Chesla et al. fails to disclose (1) a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system, or (2) event records having event data provided by the one or more monitor modules that identified the message as a threat and including the various claimed data elements (event identifier, event type, event description, etc.). The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a method of determining the number of occurrences occurring within a certain period of time (paragraph 0033); and a profiler defining old and new threats (paragraphs 0010-0011, 0014 and 0016); a method for protecting a network from an attack comprising a plurality of monitoring modules (paragraphs 0140, 0170 and 0207); and a method of analyzing an attack to the packet level, comprising Transmission Control Protocol (TCP) sequence number, Internet Protocol (IP) identification number, source port, source IP address, type of service (ToS), packet size, Internet Control

Message Protocol (ICMP) message type, destination undefined port, destination undefined IP address, destination defined port, destination defined IP address, time-to-live (TTL), and transport layer checksum. Alternatively or additionally, the traffic includes packets having payloads, and the at least one parameter includes a value of one of the packet payloads (paragraphs 0045-0046), and a controller comprising a blocking list that gives priority to addresses in the sort buffer that have the highest intensity counters (paragraph 0346).

Claims 25-26

Applicant argues that Noda does not include any monitor modules that identify threats, and does not include a database of event records based on identified threats. The Examiner respectfully disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a database of threats (paragraph 0245); an existing baseline of threats and new, detected incoming threats at a learning module that analyzes the threat (paragraph 0131).

Claims 27-29

Applicant argues that Mathews et al. does not relate to network security, and therefore does not include monitor modules that identify threats, and does not include a database of event records based on identified threats. The Examiner respectfully

disagrees. Chesla et al. discloses a method for protecting a network from an attack comprising a database of threats (paragraph 0245); an existing baseline of threats and new, detected incoming threats at a learning module that analyzes the threat (paragraph 0131).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any response to this Office Action should be faxed to (571) 273-8300 or mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Mark Fearer whose telephone number is (571) 270-1770. The Examiner can normally be reached on Monday-Thursday from 7:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Mark Fearer
M.D.F./mdf
June 18, 2008

/Ashok B. Patel/

Primary Examiner, Art Unit 2154